APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,454	08/14/2001	Liqun Chen	B-4278PCT	9593

22879   7590   05/16/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
NGUYEN, MINH DIEU T

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
05/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	09/913,454	CHEN ET AL.
	Examiner	Art Unit
	Minh Dieu Nguyen	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>09 January 2007</u>.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>44-64</u> is/are pending in the application.

    4a) Of the above claim(s) <u>1-43</u> is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>44-64</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   In view of the appeal brief filed on 1/9/2007, PROSECUTION IS HEREBY

REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the

following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply

under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed

by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and

appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth

in 37 CFR 41.20 have been increased since they were previously paid, then appellant

must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by

signing below:

Response to Arguments

2.   Applicant's arguments have been considered but are moot in view of the new

ground(s) of rejection.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

4.   Claims 52-54 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

a)   As to claim 52, at least the limitation "compare the actual module

configuration against the stored module configuration" fails to particularly point out and

distinctly claim protecting computer apparatus against modification. What happens with

the comparison result?

b)   As to claim 53, it is rejected by a similar rationale applied against claim 52.

c)   As to claim 54, at least the limitation "allow comparison between an actual

module configuration of the computer apparatus and the stored module configuration"

fails to particularly point out and distinctly claim protecting computer apparatus against

modification. What happens with the comparison result?

d)   As to claims 55-56, they are rejected by a similar rationale applied against

claim 54.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 44-47, 50 and 52-53 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Probst (5,982,899) in view of Selitrennikoff et al. (6,209,089).

a)   As to claim 44, Probst discloses a method of protecting from modification

computer apparatus (see Probst: col. 3, lines 1-3) comprising a plurality of functional

modules, wherein the computer apparatus contains or is in communication with a

trusted device adapted to respond to a user in a trusted manner, the method comprising

storing a module configuration of the computer apparatus (see Probst: col. 3, lines 8-

30); the trusted device performing a cryptographic identification process for modules

with a cryptographic identity to identify them and thereby determine an actual module

configuration (i.e. the actual module configuration is read and later compared with the

stored data, see Probst: col. 5, lines 51-53. Probst discloses a cryptographic

identification process with a cryptographic identity to determine the stored module

configuration (see Probst: Fig. 2, elements 7-11). That concept can be implemented for

determining actual module configuration for modules by a cryptographic identification

process with a cryptographic identity); the trusted device comparing the actual module

configuration against the stored module configuration (see Probst: col. 4, lines 11-14);

and the trusted device inhibiting function of the computer apparatus while the actual

module configuration does not satisfactorily match the stored module configuration (see

Probst: col. 4, lines 24-25).

Probst discloses an identifier for the entire computer system (see Probst: col. 3,

lines 62-63), however Probst is silent on a module configuration providing an

identification of each functional module in the computer apparatus.

Selitrennikoff is relied on for the teaching of a module configuration providing an identification of each functional module in the computer apparatus (see Selitrennikoff: col. 13, lines 20-24; Fig. 3, element 40).

It would be obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a module configuration providing an identification of each functional module in the computer apparatus in the system of Probst, as Selitrennikoff teaches, so as to uniquely distinguish the functional modules from one another.

b)   As to claim 45, the combination of Probst and Selitrennikoff discloses the method of claim 44, wherein the stored module configuration is held separately from the computing apparatus (i.e. over the network, see Probst: col. 3, lines 53-54).

c)   As to claim 46, the combination of Probst and Selitrennikoff discloses the method of claim 44, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process (see Probst: Fig. 2, elements 7-11).

d)   As to claim 47, the combination of Probst and Selitrennikoff discloses the method of claim 44, wherein the trusted device is adapted to communicate securely with the stored module configuration (i.e. Probst discloses the validation and authentication process with the use of public/private key, see Probst: Figs 1 and 2).

e)   As to claim 50, please see the addressed claim 44 above.

f)   As to claim 52, this claim is directed to a hardware implementation of the method of claim 44 and is rejected by a similar rationale applied against claim 44 above.

g)   As to claim 53, this claim is directed to a hardware implementation of the

method of claims 45-46 and is rejected by a similar rationale applied against claim 45-

46 above.

7.   Claims 48-49, 54-63 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Probst (5,982,899) in view of in view of Selitrennikoff et al. (6,209,089) and further

in view of Herzi et al. (6,353,885).

a)   As to claims 48 and 49, the combination of Probst and Selitrennikoff

discloses the method of claim 47, however it is silent on the capability of the stored

module configuration is stored in a security token and wherein the security token is a

smart card.

Herzi is relied on for the teaching of having the stored module configuration is

stored in a security token and wherein the security token is a smart card (i.e. stored

module configuration contains BIOS level settings is stored in a smart card, see Herzi:

col. 3, lines 54-57; col. 3, lines 5-13).

It would be obvious to one of ordinary skill in the art at the time of the invention to

employ the use of having a security token adapted to hold a stored module

configuration of modules in a computer apparatus in the system of Probst and

Selitrennikoff, as Herzi teaches so as to flexibly provide a computer configuration in a

multi-user computer system environment (see Herzi: col. 2, lines 3-5).

b)   As to claim 54, as best understood, Probst discloses the stored module

configuration is stored in a computer apparatus (see Probst: col. 3, lines 28-31) and

adapted to provide the stored module configuration to the computer apparatus to allow

comparison between an actual module configuration of the computer apparatus and the

stored module configuration (see Probst: Fig. 2).

Probst discloses an identifier for the entire computer system (see Probst: col. 3,

lines 62-63), however Probst is silent on a module configuration providing an

identification of each functional module in the computer apparatus.

Selitrennikoff is relied on for the teaching of a module configuration providing an

identification of each functional module in the computer apparatus (see Selitrennikoff:

col. 13, lines 20-24; Fig. 3, element 40).

It would be obvious to one of ordinary skill in the art at the time of the invention to

employ the use of having a module configuration providing an identification of each

functional module in the computer apparatus in the system of Probst, as Selitrennikoff

teaches, so as to uniquely distinguish the functional modules from one another.

The combination of Probst and Selitrennikoff is silent on the capability of having a

security token adapted to hold a stored module configuration of modules in a computer

apparatus.

Herzi is relied on for the teaching of having a security token adapted to hold a

stored module configuration of modules in a computer apparatus (i.e. stored module

configuration contains BIOS level settings is stored in a smart card, see Herzi: col. 3,

lines 54-57; col. 3, lines 5-13).

It would be obvious to one of ordinary skill in the art at the time of the invention to

employ the use of having a security token adapted to hold a stored module

configuration of modules in a computer apparatus in the system of Probst and

Selitrennikoff, as Herzi teaches so as to flexibly provide a computer configuration in a

multi-user computer system environment (see Herzi: col. 2, lines 3-5).

    c)   As to claim 55, the combination of Probst, Selitrennikoff and Herzi

discloses a security token of claim 54, wherein the stored module configuration is stored

in an encrypted form (see Probst: Fig. 1, element 5).

    d)   As to claim 56, the combination of Probst, Selitrennikoff and Herzi

discloses a security token of claim 54, wherein the security token is a smart card (see

Herzi: Fig. 1, element 28).

    e)   As to claim 57, Probst discloses a method of protecting from modification

computer apparatus (see Probst: col. 3, lines 1-3) comprising a plurality of functional

modules, wherein the computer apparatus contains or is in communication with a

trusted device adapted to respond to a user in a trusted manner, the method comprising

storing a module configuration of the computer apparatus (see Probst: col. 3, lines 8-

30); checking an actual module configuration against the stored module configuration

(see Probst: col. 4, lines 11-14); and inhibiting function of the computer apparatus if the

actual module configuration does not satisfactorily match the stored module

configuration (see Probst: col. 4, lines 24-25).

    Probst discloses an identifier for the entire computer system (see Probst: col. 3,

lines 62-63), however Probst is silent on a module configuration providing an

identification of each functional module in the computer apparatus.

Selitrennikoff is relied on for the teaching of a module configuration providing an

identification of each functional module in the computer apparatus (see Selitrennikoff:

col. 13, lines 20-24; Fig. 3, element 40).

It would be obvious to one of ordinary skill in the art at the time of the invention to

employ the use of having a module configuration providing an identification of each

functional module in the computer apparatus in the system of Probst, as Selitrennikoff

teaches, so as to uniquely distinguish the functional modules from one another.

The combination of Probst and Selitrennikoff is silent on the capability of storing

a module configuration of the computer apparatus on a security token removably

attachable to the computer apparatus.

Herzi is relied on for the teaching of storing a module configuration of the

computer apparatus on a security token removably attachable to the computer

apparatus (i.e. stored module configuration contains BIOS level settings is stored in a

smart card, see Herzi: col. 3, lines 54-57; col. 3, lines 5-13).

It would be obvious to one of ordinary skill in the art at the time of the invention to

employ the use of having a security token adapted to hold a stored module

configuration of modules in a computer apparatus in the system of Probst and

Selitrennikoff, as Herzi teaches so as to flexibly provide a computer configuration in a

multi-user computer system environment (see Herzi: col. 2, lines 3-5).

f)   As to claim 58, the combination of Probst and Selitrennikoff discloses the

method of claim 57, wherein the stored module configuration is stored such that it is

accessible only by a cryptographic authentication process (see Probst: Fig. 2, elements 7-11).

g)   As to claim 59, please see the addressed claim 57 above.

h)   As to claim 60, the combination of Probst, Selitrennikoff and Herzi discloses the method of claim 59, wherein the trusted device is adapted to communicate securely with the stored module configuration (i.e. Probst discloses the validation and authentication process with the use of public/private key, see Probst: Figs 1 and 2).

i)   As to claims 61-63, please see the addressed claim 57 above.

8.   Claims 51 and 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Probst (5,982,899) in view of Selitrennikoff et al. (6,209,089) in view of Herzi et al. (6,353,885) and further in view of Muftic (5,943,423).

Probst discloses the module configuration is held by a remote module validation authority, however the combination of Probst, Selitrennikoff and Herzi is silent on the capability of the remote validation authority provides a service allowing a replacement security token to be provided if a security token is lost or stolen.

Muftic is relied on for the teaching of a service allowing a replacement security token to be provided if a security token is lost or stolen (col. 6, lines 50-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of replacing lost or stolen security token as Muftic teaches in the system of Probst, Selitrennikoff and Herzi so as not to disrupt the smart card services.
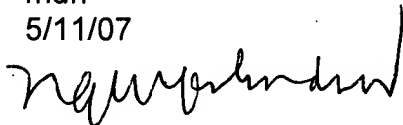
Conclusion

9.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-

3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number

for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

mdn
5/11/07

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137